Data processing device and operating method for preventing a differential current consumption analysis.

The invention relates to a method of operating a data processing device, notably a chip card, which includes an integrated circuit which executes useful arithmetic operations, notably cryptographic operations, in dependence on a first clock signal as disclosed in the introductory part of Claim 1. The invention also relates to a data processing device, notably a chip card, which is specifically intended to carry out the method and includes an integrated circuit which executes useful arithmetic operations, notably cryptographic operations, in dependence on a first clock signal as disclosed in the introductory part of Claim 6.

In many data processing apparatus provided with an integrated circuit, for example, cryptographic operations are carried out so as to protect the operation of such apparatus or the data transported in the apparatus. The arithmetic operations required for this purpose are carried out by standard processors as well as by dedicated crypto processors. A typical example of the latter processor is formed by a chip card or an IC card. Data or intermediate results used in this context customarily constitute security-relevant information such as, for example, cryptographic keys or operands.

The arithmetic operations performed by the integrated circuit, for example in order to calculate cryptographic algorithms, involve the formation of logic combinations of operands or intermediate results. Depending on the technology used, such operations, notably the loading of empty or previously erased storage sections or registers with data, lead to an increased current consumption of the data processing apparatus. In the case of complementary logic, for example CMOS, an increase of the current consumption occurs when the value of a bit storage cell changes, i.e. when its value changes from "0" to "1" or from "1" to "0". The increase of the consumption is then dependent on the number of bit positions changed in the memory or register. In other words, the loading of a previously erased register causes an increase of the current consumption which is proportional to the Hamming weight of the operand (= number of bits having the value "1") written into the empty register. Analysis of this current variation could thus enable extraction of information

concerning the operations executed, thus enabling successful crypto analysis of secret operands such as, for example, cryptographic keys. When several current measurements are performed on the data processing apparatus, adequate information could be extracted, for example in the case of very small signal variations. On the other hand, a plurality of current measurements could also enable a possibly required differentiation. This type of crypto analysis is also called "Differential Power Analysis" whereby an outsider could successfully perform a possibly unauthorized crypto analysis of the cryptographic operations, algorithms, operands or data purely by observing changes in the current consumption of the data processing apparatus. "Differential Power Analysis" thus enables the extraction of additional internal information of an integrated circuit beyond pure functionality.

US 4,813,024 discloses an integrated circuit for the storage and processing of secret data wherein a memory includes a simulation storage cell whose current consumption is identical to that of a storage cell which has not been programmed thus far. Fluctuations in the current and the voltage are thus substantially but not completely eliminated. This system is also very complex and expensive.

EP 0 482 975 B1 discloses a memory card which includes a microcircuit and at least one memory which is connected to a data processing member, the data processing member being controlled by a data signal from outside the card and delivering a command transmission signal in response to said data signal at a given instant, said command transmission signal being delayed by a predetermined period of time (T) relative to the reception of the data signal, the period of time (T) being selected so as to be variable in time on a random basis in order to enhance the security. Thus, a period of time elapsing between the reception of an external signal and a response is subject to a random generator and is not suitable for evaluation for the purpose of extraction of secret data. Crypto analysis on the basis of a current variation during the writing of the memory or the execution of arithmetic operations, however, cannot be precluded by such a system.

EP 0 507 669 A1 discloses a card for electronic payment, i.e. a so-called paycard, in which each pay unit comprises a plurality of bits instead of only a single bit, the additional bits numbering the pay units in a random series and being derived from a random number series. This random number series is available to sales outlets accepting a paycard. However, this system again is not capable of precluding crypto analysis on the basis of a current variation occurring during the writing of the memory or the execution of arithmetic operations.

FR 2 693 014 B1 describes a device for evaluating chip cards, for example a public telephone, which determines, by way of a capacitance measurement, whether external apparatus is connected to an inserted chip card.

It is an object of the present invention to provide an improved method and an improved data processing device of the kind set forth which eliminate the described drawbacks and offer effective protection against "Differential Power Analysis".

This object is achieved by means of a method of the kind set forth which is characterized as disclosed in Claim 1, and by means of a data processing device of the kind set forth which is characterized as disclosed in Claim 6.

To this end, in conformity with the method of the kind set forth according to the invention a second clock signal is derived from the first clock signal under random control so as to be applied to the integrated circuit instead of the first clock signal while distances between clock edges of the second clock signal vary at random in time.

This offers the advantage that the execution in time of useful arithmetic operations is distorted independently of data processed in the data processing device, so that a share of the power consumption of the integrated circuit which is characteristic of a useful arithmetic operation or operations is disguised and can no longer be analyzed by means of "Differential Power Analysis".

Preferred further versions of the method are described in the Claims 2 to 5.

In order to disguise a characteristic share of the current consumption of the integrated circuit which is due to calculations or useful operations of the integrated circuit even further, the integrated circuit is switched to different modes of operation under random control.

In order to prevent reproducibility of the characteristic share of the current consumption which is due to identical useful operations, the different modes of operation involve at least two calculation methods which produce an identical result while using different approaches.

In order to disguise the type and time of the useful arithmetic operations even further, the different modes of operation include at least one "dummy" mode in which the integrated circuit executes dummy arithmetic operations instead of useful operations, said dummy operations processing predetermined input data or random input data, the result being rejected and not taken up in the results or input data for the useful arithmetic operations.

Optionally, there is provided an additional mode of operation "deactivated" in which the integrated circuit does not execute arithmetic operations.

A data processing device of the kind set forth according to the invention is provided with a clock control unit which is connected to the integrated circuit as well as with a random generator which is connected to the clock control unit, the clock control unit being constructed in such a manner that it generates a second clock signal in dependence on the random generator and the first clock signal, which second clock signal varies at random and controls the integrated circuit.

This offers the advantage that the execution in time of useful arithmetic operations is distorted independently of data processed in the data processing device, so that a share of the current consumption of the integrated circuit which is characteristic of the useful arithmetic operations is disguised and can no longer be analyzed by way of "Differential Power Analysis".

Further preferred embodiments of the data processing device are described in the Claims 7 to 10.

The invention will be described in detail hereinafter with reference to the accompanying drawings. Therein

Fig. 1 shows a block diagram of a preferred embodiment of a data processing device according to the invention, and

Fig. 2 graphically illustrates various signals generated and used in the data processing device.

Fig. 1 shows a preferred embodiment of a data processing device 100 according to the invention which includes an integrated circuit 10, a random generator 12 and a clock control unit 14. The integrated circuit 10 carries out useful arithmetic operations to be described hereinafter. Useful arithmetic operations are arithmetic operations which process input data in a desired manner and produce a desired result or intermediate result. An example in this respect is a predetermined arithmetic method involving cryptographic operations and executed in dedicated crypto processors. Such a predetermined arithmetic method will be referred to as the method 1 or the first mode of operation hereinafter.

Fig. 2 shows, as a function of time t, various signals which are generated in the data processing unit 100 and are plotted on a horizontal axis 16. The reference numeral 18 denotes a signal $TAKT_1$ which controls the clock control unit 14 via a lead 19. The reference numeral 20 denotes a signal $TAKT_2$ which is generated by the clock control unit 14 and is applied to the integrated circuit 10 via a lead 21. The reference numeral 22 denotes a signal DUMMY whereas the reference numeral 24 denotes a signal DEAKT and the reference numeral 26 denotes a signal ALT, said signals being applied, via control leads 28, from the clock control unit 14 to the integrated circuit 10 in order to control the latter. An additional line 29 shows the instantaneous mode of operation of the integrated circuit 10 under the control of the clock control unit 14. The reference numeral 30 denotes a mode of operation "method 1", whereas the reference numeral 32 denotes a mode of operation "dummy", the reference 34 denotes a mode of operation "method 2" and the reference numeral 36 denotes a mode of operation "deactivated". These modes of operation 30, 32, 34 and 36 and their functions will be described in detail hereinafter.

According to an article "Differential Power Analysis" published by Paul Kocher on the Internet under http://www.cryptography.com/dpa not only the input/output signals are analyzed but also a current consumption I_a or voltage drops ΔU_a of a supply voltage U_a of the integrated circuit. The success of this method of analysis is dependent on whether a number N_A of analog ($I_a(t)$ or $\Delta U_a(t)$) signal variations S(k,t) in time can be measured with $k = \{1,...,N_A\}$ different operands in such a manner that it is possible to form a sum of the form:

$$T(i,t) = \sum_{k=1}^{N_A} p(i,k).S(k,t)$$

with the coefficients p(ik), where $i = \{0,1,2,...\}$. When different signal variations $S(k_1,t_1)$, $S(k_2,t_1)$, $S(k_3,t_1)$ ... are observed at the same instant $t = t_1$, differential power analysis can be successful only if the integrated circuit executes the same arithmetic operation with different operands $k = \{1,...,N_A\}$ at that instant, i.e. it must be possible to make the signal variations S(k,t) register exactly. This holds not only for the calculation itself, but also for the input and output of data.

The invention prevents such "registration" in that the integrated circuit 10 is controlled by the random controlled clock control unit 14. Moreover, the integrated circuit not only has the mode of operation "method 1" 30, but also the mode of operation "dummy"

32 in which dummy calculation operations to be described hereinafter are executed, the mode of operation "deactivated" 36 in which the integrated circuit 10 does not execute arithmetic operations and results or intermediate results formed thus far are possibly stored, and the mode of operation "method 2" 34 in which the useful arithmetic operations of the "method 1" 30 are executed by means of an alternative method; the result thereof is not different from that of the first mode of operation "method 1" 30 but is merely calculated in a different way, so that in comparison with the "method 1" 30 the "method 2" 34 involves a different variation of the input current I_a or different voltage variations ΔU_a of the integrated circuit 10 for the same operands k.

Dummy arithmetic operations are arithmetic operations which act on predetermined input data or input data selected at random, the result being rejected and not being taken up in the results or the input data for the useful arithmetic operations.

The clock control unit 14 is controlled, via the lead 19, by the signal $TAKT_1$ 18 as well as by the random generator 12 via the lead 38. The clock control unit 14 generates a random clock signal $TAKT_2$ 20 from $TAKT_1$ 18 and the input from the lead 38, which clock signal $TAKT_2$ 20 distorts the time axis 16 in S(k,t) independently from the data calculated in the integrated circuit 10. This makes it impossible to perform the above-mentioned summing with the desired result for the differential power analysis.

Furthermore, from one clock edge until a later clock edge the control signals DUMMY 22, DEAKT 24 and ALT 26 are set on the control leads 28, in dependence on the random generator, in the manner shown in Fig.2. During the signal DUMMY 22 the integrated circuit 10 operates in the mode "dummy" 32; in the presence of the signal DEAKT 24 the integrated circuit 10 operates in the mode "deactivated" 36, whereas in the presence of the signal ALT 26 the integrated circuit 10 operates in the mode "method 2" 34, whereas if no signal is present on the control leads 28, the integrated circuit 10 operates in the mode "method 1" 30 as is demonstrated by the line 29 in Fig. 2 which illustrates the modes of operation.

The mode of operation "dummy" 32 disguises the actual calculation S(k,t). It is possible to provide several, different modes of operation "dummy n" with corresponding, different signals "DUMMY n". It is particularly advantageous when the instant and duration of the dummy signals are not determined by the integrated circuit 10 to be protected itself, but by the external devices consisting of the random generator 12 and the clock control unit 14. In the mode of operation "deactivated" 36, the time axis 16 is additionally distorted further so that the above-mentioned formation of the sum for the "Differential Power

Analysis" is additionally impeded or made impossible. In the mode of operation "method 2" 34 the calculation is further disguised, so that the calculation S(k,t) is difficult to identify. If desired, further, different modes of operation with a different calculation approach "method n" are provided and also associated signals "ALT n".

Summarizing it can be said that according to the invention a characteristic share of the current consumption of the integrated circuit 10 is not eliminated but disguised. To this end, different methods of disguise are flexibly combined by means of the clock control unit 14. To some extent dummy signals are generated by dummy calculations which cannot be recognized as such from the outside, because they are generated on a random basis.